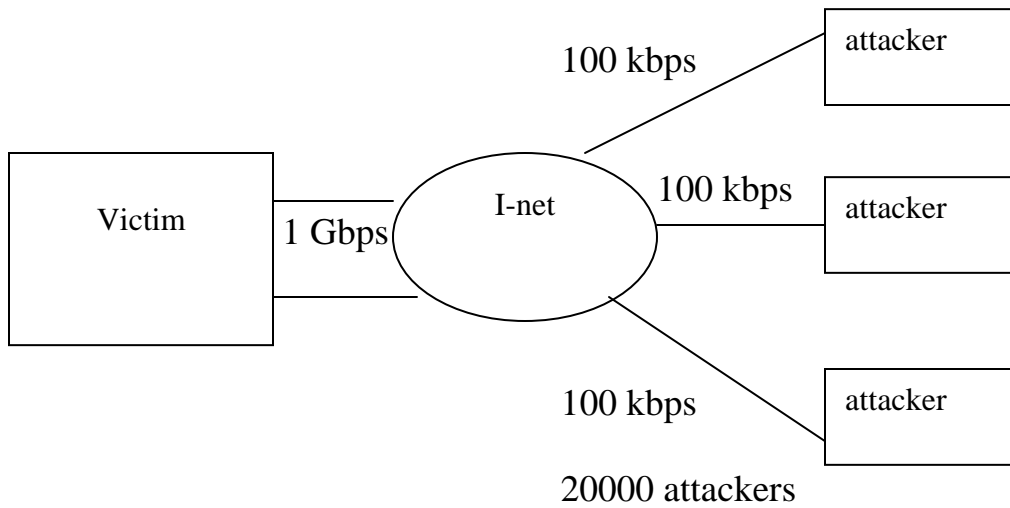


Class Note for CSE 509 (4/17)

Denial of Service Attacks

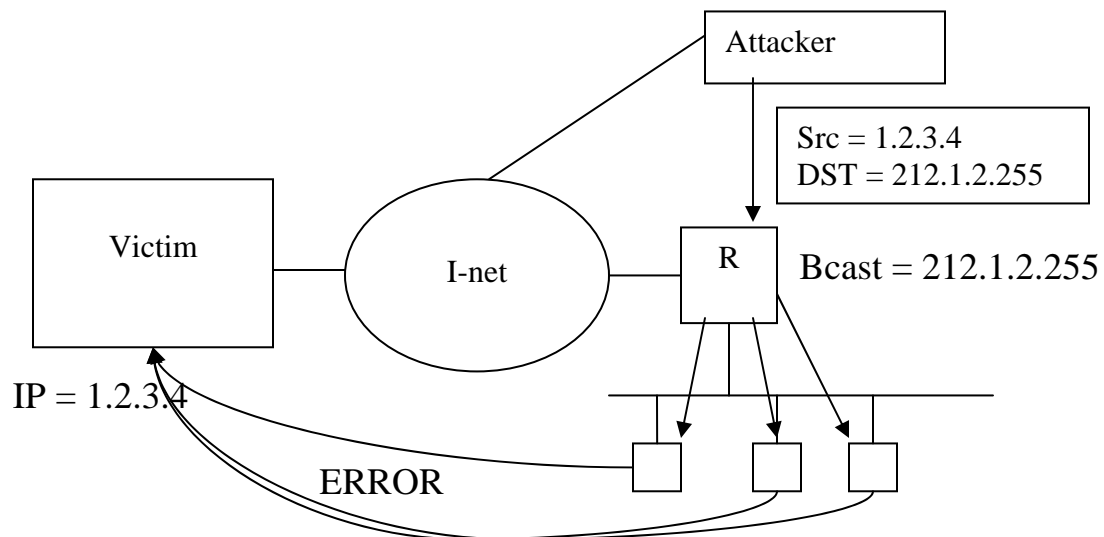
- Crashing program
- Resource exhaustion
 - o Network bandwidth
 - o Memory
 - o OS resources
 - o Disk
 - o CPU

1. Some network Dos attacks



more attacker machines → hard to distinguish attackers

2. Smurf attack



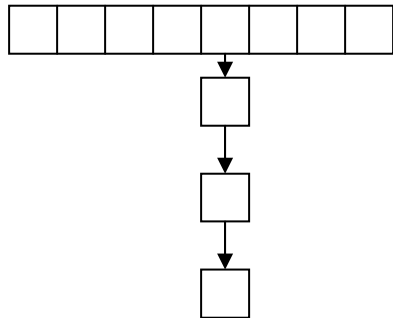
3. CPU Dos

- Algorithmic complexity Attacks

- o Example : Hash Tables

$i = \text{hash}(x)$

$\text{append}(\text{bucket}[i], x)$



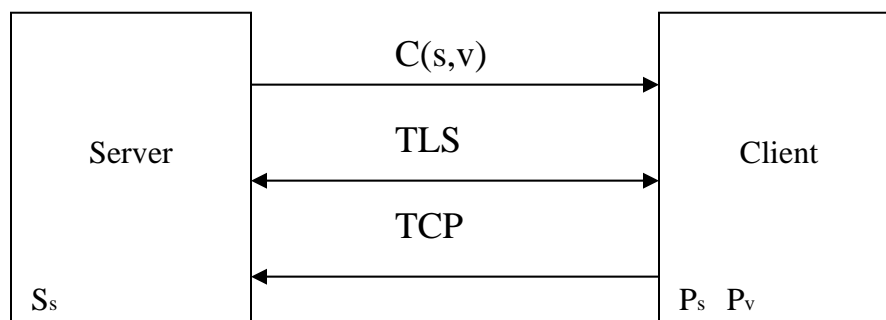
hash function is typically fixed and public

→ easy for an attacker to find collisions.

Attack (input: x_1, \dots, x_n)

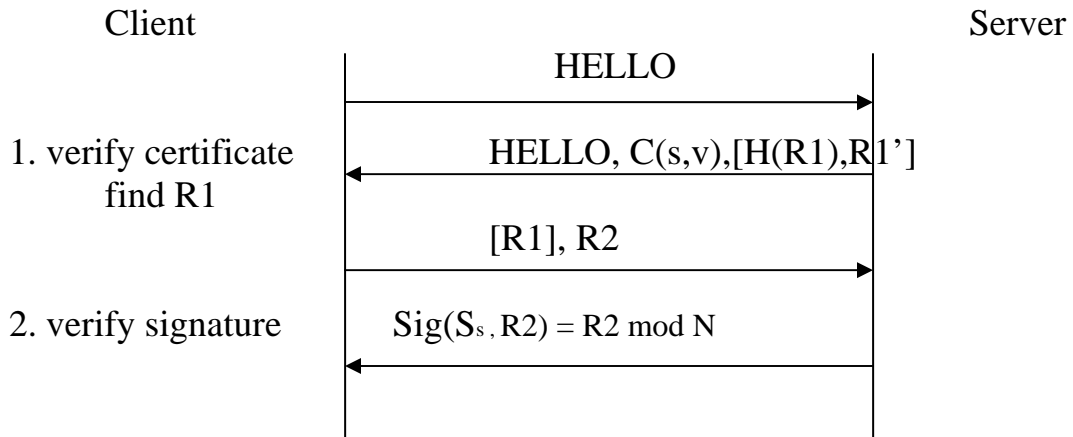
- 1). Choose many inputs that all hash to 0
- 2). Interact w/ server to cause it to insert x_1, \dots, x_n into its hash table
- 3). Force server to do hash table lookups

4. TLS/SSL



TLS guarantees

- o secrecy
- o authenticity
- o server identity



- modular exponentiation is slow
- typical Desktop == 100 sig/sec

Client puzzles

- problems
 - o Does not distinguish real from attacks
 - o Must be configured / system

CPU puzzles vs memory puzzles

	CPU	Memory
TOP end machine	3 GHz	2 GB
Phone	.1 GHz	128MB
	<30>	<16>